

***Remarks***

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1-40 are pending in the application, with claims 1, 7, 15, 16, 23, 24, 29, and 30 being the independent claims. Claims 1, 4-8, 10-16, 19-24, 26-31, and 33-40 are sought to be amended for clarity.

These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and following remarks, Applicants respectfully request that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

***Examiner's Response to Arguments:***

The Examiner, in response to Applicants' previous arguments, on page 3 of the Office Action states:

The Timson prior art discloses the capability to add additional authentication modules to the authentication procedures. These additional authentication modules can generate a hierarchical structure for the authentication process with access to the resolution authority performed as a last authentication process as per claim limitation. (see Timson col. 4, line 60- col. 5, line 4: hierarchical authorization structure)...

Applicants respectfully disagree. As discussed previously, in the reply filed January 4, 2008, Timson discloses an apparatus and a method for providing access to secured data or area that includes at least two secure data modules, an interrogatable module (IM) and an enable module (EM). ***In the case that EM does not have appropriate permissions, no data communication is allowed and also if the EM does***

*not provide the necessary permissions, the IM prevents the EM to access the requested data* (Timson column 3, line 11 to column 4, line 15, and also column 13, line 22 to column 14, line 40). Therefore, the apparatus and method of Timson prevents access to the secured data or prevents any data communication in response to the comparisons that indicate that either the EM or the IM do not have necessary permissions.

Moreover, Timson discloses that a set of data operations may be stored on a controllable module. Other types of modules such as EM or IM can be made from the controller module by writing permissions data to the modules. In this manner, *hierarchical sets of permissions* for data operations can be written to the modules. However, an enabling module cannot empower another module with more permissions than the enabling module itself contains (Timson Col. 4, Line 60 to Col. 5, Line 4). Therefore, Timson teaches that only permissions can be hierarchical not the authentication process as the Examiner states in the Office Action. The authentication process of Timson only involves one EM and one IM that communicate with each other to provide access to secured data and if EM or IM does not have the necessary permissions, access to the secured data is denied. However, the sets of permissions of the modules can be hierarchical. Therefore, Applicants maintain that Timson does not teach or suggest a hierarchical structure for authentication process.

***Rejections under 35 U.S.C. § 103***

**Claims 1-4, 7-10, 14, 16-19, 24-26, 29-33, and 37-40**

The Examiner rejected claims 1-4, 7-10, 14, 16-19, 24-26, 29-33, and 37-40 under 35 U.S.C. § 103(a) as allegedly being anticipated by U.S. Patent No. 6,041,412 to Timson *et al.* ("Timson") in view of U.S. Patent No. 6,959,336 to Moreh *et al.* ("Moreh"). Applicants respectfully traverse this rejection.

**Claims 1-4, 16-19, 24-26, 29, and 38-40**

The Examiner contends that the combination of Timson and Moreh teaches each of the elements of independent claims 1, 16, 24, and 29. Applicants respectfully disagree. Claim 1, as amended, recites:

A method for providing an access candidate access to secured electronic data, the method comprising:  
receiving a request for access candidate access to the secured electronic data by a controller associated with the secured electronic data;  
comparing, at the controller, one or more attributes of the access candidate with one or more access requirements associated with the secured electronic data;  
***submitting, by the controller, a request for authorization to a resolution authority, which is configured to modify the one or more access requirements, in response to a comparison that indicates that access by the access candidate is prohibited; and***  
granting the access candidate access to the secured electronic data if the resolution authority provides authorization for such access.

Applicants maintain that the combination of Timson and Moreh does not teach or suggest each and every feature of claim 1, as amended. For example, the combination of Timson and Moreh does not teach or suggest "*submitting, by the controller, a request for authorization to a resolution authority, which is configured to modify the one or more*

*access requirements, in response to a comparison that indicates that access by the access candidate is prohibited"* as recited in claim 1, as amended.

The Examiner, on page 6 of the Office Action, states that Timson does not disclose a resolution authority. However, the Examiner relies upon Moreh (Moreh Col. 2, Lines 48-62; Col. 5, Line 56 to Col. 6, Line 19) to allegedly show the resolution authority feature of claim 1:

Timson discloses the generation of a hierarchical structure for access determination such as additional authorization module. (see Timson col. 4, line 60 - col. 5, line 4: hierarchical authorization structure) Timson does not specifically disclose a resolution authority or a 3<sup>rd</sup> party providing authentication services. However, Moreh discloses a resolution authority. (see Moreh col. 2, lines 48-62; col. 5, line 56 - col. 6, line 19: authentication service between client and server using intermediate entity (protocol proxy))

Applicants maintain that the combination of Timson and Moreh fails to teach all the elements of claim 1 and similarly worded claims 16, 24, and 29 for at least the following reasons. For example, using similar language, claims 1, 16, 24, and 29 all require submitting, by the controller, a request for authorization to a resolution authority, which is configured to modify the one or more access requirements, in response to a comparison that indicates that access by the access candidate is prohibited.

As discussed previously, in the reply filed January 4, 2008, Timson discloses an apparatus and a method for providing access to secured data or area that includes at least two secure data modules, an interrogatable module (IM) and an enable module (EM). ***In the case that EM does not have appropriate permissions, no data communication is allowed*** and also ***if the EM does not provide the necessary permissions, the IM prevents the EM to access the requested data*** (Timson Col. 3, Line 11 to Col. 4, Line 15, and also

Col. 13, Line 22 to Col. 14, Line 40). Therefore, the apparatus and method of Timson prevents access to the secured data or prevents any data communication in response to the comparisons that indicate that either the EM or the IM do not have necessary permissions.

Furthermore, Moreh discloses a system and a method to efficiently maintaining security in information systems when multiple authentication types and sources are used (Moreh Col. 1, Lines 17-19). The advantage of the method of Moreh is that it permits multiple authentication types and sources by effectively abstracting these (Moreh Col. 2, Lines 63-65). In the method of Moreh, a *subject*, who must authenticate itself, uses a *client* (in a client domain) to initiate the process of obtaining access to a server application. The client contacts an *authorization agent* (in an agent domain) and passes the name of the subject and their domain. The authentication agent uses a *mechanism resolution process* to determine an appropriate authentication mechanism for the client. If more than one appropriate mechanism exists, the authentication agent uses its protocol with the client to resolve to exactly one authentication mechanism. The mechanism resolution process uses a *mechanism repository* to retrieve information about the appropriate authentication mechanism. The client communicates an authentication request for access to the server application to a protocol proxy. The protocol proxy translates the authentication request into the native protocol of the authentication mechanism and communicates the translated request to the authentication mechanism. Upon successful authentication, the protocol proxy receives a response from the authentication mechanism including attributes and access rights of the subject. Then the protocol proxy creates a name assertion, translate this into an authentication response,

and transmits it back to the client. The client delivers the authentication response to the server application.

Therefore, the protocol proxy of Moreh is only used between the client and the authentication mechanism to authenticate the client and create from the client credentials an authentication name assertion allowing the client to access the server application (Moreh Col. 2, Lines 57-62). This is not the same as *submitting, by the controller, a request for authorization to a resolution authority, which is configured to modify the one or more access requirements, in response to a comparison that indicates that access by the access candidate is prohibited*, as recited in claim 1 and similarly worded claims 7, 24, and 29. The protocol proxy of Moreh authenticates the client and *upon the successful authentication* creates the authentication name assertion to allow the client to access the server application. In contrast, claim 1 recites that in response to a comparison that indicates that access by the access candidate is prohibited, the controller submits a request for authorization to a resolution authority, which is configured to modify the one or more access requirements.

Moreover, the interrogatable module (IM) and the enable module (EM) of Timson and protocol proxy of Moreh are directed to only authenticate the user and they do not have the ability to modify any access requirements. In contrast, claim 1 recites that the authorization authority has the ability to modify the one or more access requirements that are associated with secured data.

Therefore, for at least the above reasons, the combination of Timson and Moreh fails to disclose all features of independent claim 1, as amended. Independent claims 7, 24, and 29, as amended, are patentable for similar reasons.

In addition, the Examiner rejected claims 2-4, 18, 19, 25, 26, and 38-40 as being anticipated by the combination of Timson and Moreh. These dependent claims necessarily include all features of claims 1, 16, and 24. As discussed above, the combination of Timson and Moreh fails to disclose all features of claims 1, 16, 24, and 29, therefore claims 2-4, 18, 19, 25, 26, and 38-40 are not anticipated by the cited reference.

Also, Applicants assert the dependent claims 38-40 are patentable over the applied references in view of their additional combinations of distinguishing features. For example, the "granting a waiver of the one or more access requirements associated with the secured electronic data" feature recited in claim 38, the "modifying the one or more access requirements associated with the secured electronic data" feature recited in claim 39, and the "excluding the electronic data assigned to one or more prohibited data classes from access by the access candidate" feature recited in claim 40 are not explicitly or implicitly taught or suggested by the applied references. In contrast, in the case where there is conflict between EM or IM's permissions and the requirements, Timson's system prevents data communication or data access. There is absolutely no attempt to resolve the conflict in Timson's system. Moreover, the protocol proxy of Moreh only authenticates the client and in case of a successful authentication, creates an authentication name assertion allowing the client to access the server application. Further, the Examiner fails to specifically point out the portions of Moreh that the Examiner alleges that show the above-noted features of claims 38-40.

**Claims 7-10, 14, 30-33, and 37**

The Examiner rejected independent claims 7 and 30 as likewise being anticipated by the combination of Timson and Moreh. These independent claims contain similar language to claims 1, 16, 24 and 29 and are patentable for the same reasons discussed above. Dependent claims 8-10, 14, 31-33 and 37 necessarily include all features of claims 7 and 30 respectively. The combination of Timson and Moreh fails to disclose all features of claims 7 and 30, therefore claims 8-10, 14, 31-33 and 37 are not anticipated by the combination of Timson and Moreh.

**Claims 5, 6, 11-13, 15, 20-23, 27, 28, and 34-36**

The Examiner rejected claims 5, 6, 11-13, 15, 20-23, 27, 28, and 34-36 under 35 U.S.C. § 103(a) as allegedly being unpatentable over Timson in view of Moreh and further in view of U.S. Patent Publication No. 2004/0049687 to Orsini *et al.* ("Orsini"). Applicants respectfully traverse this rejection.

Independent claims 15 and 23 contain similar language to claims 1, 7, 16, 24 and 29 and are patentable over the combination of Timson and Moreh for the same reasons discussed above. Further, Orsini fails to cure the deficiencies of the combination of Timson and Moreh as noted above. Orsini does not teach what is missing from the combination of Timson and Moreh, for example the resolution authority, which is configured to modify access requirements (as is disclosed in claims 15 and 23). Therefore, claims 15 and 23 are patentable over Timson, Moreh, and Orsini taken alone, or in combination, for at least the reasons provided above.



In addition, the Examiner rejected claims 5, 6, 11-13, 20-22, 27, 28, and 34-36 as allegedly being unpatentable over the combination of Timson and Moreh and further in view of Orsini. These dependent claims necessarily include all features of claims 1, 7, 16, 24, and 30, respectively. As discussed above, the combination of Timson and Moreh fails to disclose all features of claims 1, 7, 16, 24, and 30, and further, Orsini fails to cure the deficiencies of the combination of Timson and Moreh as noted above. Therefore claims 5, 6, 11-13, 20-22, 27, 28, and 34-36 are patentable over Timson, Moreh, and Orsini taken alone, or in combination, for at least the reasons provided above.

***Conclusion***

Applicants submit that all of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicants therefore respectfully request that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicants believe that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.



Glenn J. Perry  
Attorney for Applicants  
Registration No. 28,458

Date: 2 July 2008

1100 New York Avenue, N.W.  
Washington, D.C. 20005-3934  
(202) 371-2600

809500\_2.DOC